Draft

Frequently Asked Questions (FAQs)

FAQ 8: Access

ACCESS PRINCIPLE*:*

Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the legitimate rights of persons other than the individual would be violated.

---

1. Q: Is the right of access absolute?

1. A: No. Under the safe harbor principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. Nonetheless, the obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), thenconsistent with the other provisions of these FAQs, the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., non-sensitive marketing data that is used to determine whether or not to send the individual a catalog), but is readily available and inexpensive to provide, ~~on~~ an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be denied in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

2. Q: What is confidential commercial information and may organizations deny access in order to safeguard it?

2. A: Confidential commercial information (as that term is used in the Federal Rules of Civil Procedure on discovery) is information which an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. The particular computer program an organization uses, such as a modeling program, or the details of that program may be confidential commercial information. ~~For example, w~~Where confidential commercial information can be readily separated from other information subject to an access request, the organization

should redact the confidential commercial information and make available the non-confidential information. Organizations may deny or limit access to the extent that granting it would reveal its own confidential commercial information as defined above, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another where such information is subject to a contractual obligation of confidentiality in circumstances where such an obligation of confidentiality would normally be undertaken or imposed.

3. Q: In providing access, may an organization disclose to individuals personal information about them derived from its data bases or is access to the data base itself required?

3. A: Access can be provided in the form of disclosure by an organization to the individual and does not require access by the individual to an organization's data base.

4. Q: Does an organization have to restructure its data bases to be able to provide access?

4. A: Access needs to be provided only to the extent that an organization stores the information. The access principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

5. Q: *These replies make clear that access may be denied in certain circumstances. In what other circumstances may an organization deny individuals access to their personal information?*

5. A: Such circumstances are limited, and any reasons for denying access must be specific. An organization can refuse to provide access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defence; or public security. In addition, where personal information is processed *solely* **for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:**

a. interference with execution or enforcement of the law, including the prevention, investigation or detection of offences or the right to a fair trial;

b. interference with private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial;

c. disclosure of personal information pertaining to other individual(s) where such references cannot be redacted;

d. breaching a legal or other professional privilege or obligation;

e. breaching the necessary confidentiality ~~(in contexts where confidentiality is normally expected or imposed);~~

~~f. prejudicing~~ offuture or ongoing negotiations, such as those involving ~~company acquisitions;~~

~~g. breaching an express or implied promise (in contexts where confidentiality is normally expected) that evaluative or opinion material (or the identity of the person who supplied it or both) would be held in confidence;~~

~~h.~~ the acquisition of publicly quoted companies;

f. prejudicing employee security investigations or grievance proceedings;

~~i.~~

g. prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations; ~~or~~
~~j. impeding the~~ or

h. prejudicing the confidentiality that may be necessary in connection with monitoring, inspection or regulatory functions connected with sound economic or financial management; or

i.
~~k.~~ other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. ~~as set forth in the principle.~~

An organization which claims an exception has the burden of demonstrating its applicability (as is normally the case). As noted above,

the reasons for denying or limiting access and a contact point for further inquires should be given to individuals.

6. Q: Can an organization charge a fee to cover the cost of providing access?

6. A: Yes. The OECD Guidelines recognize that organizations may charge a fee, provided that it is not excessive. Thus organizations may charge a reasonable fee for access. Charging a fee may be useful in discouraging repetitive and vexatious requests.

Organizations that are in the business of selling publicly available information may thus charge the organization's customary fee in responding to requests for access. Individuals may alternatively seek access to their information from the organization that originally compiled the data.

7. Q: Is an organization required to provide access to personal information derived from public records?

7. A: To clarify first, public records are those records kept by government agencies or entities at any level that are open to consultation by the public in general. It is not necessary to apply the access principle to such information as long as it is not combined with other personal information, apart from when small amounts of non-public record information are used for indexing or organizing public record information. However, any conditions for consultation established by the relevant jurisdiction are to be respected. Where public record information is combined with other non-public record information (other than as specifically noted above), however, an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

8. Q: Does the access principle have to be applied to publicly available personal information?

8. A: As with public record information (see Q7), it is not necessary to provide access to information that is alreadypublicly available to the public at large, as long as it is not combined with non-publicly available information.

9. Q: How can an organization protect itself against repetitious or vexatious requests for access?

9. A: An organization does not have to respond to such requests for access. For these reasons, organizations may charge a reasonable fee and may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

10. Q: How can an organization protect itself against fraudulent requests for access?

10. A: An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

11. Q: Is there a time within which responses must be provided to access requests?

11. A: Yes, organizations should respond without excessive delay and within a reasonable time period. This requirement may be satisfied in different ways as the explanatory memorandum to the 1980 OECD Privacy Guidelines states. For example, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests.

~~**Please note: Sector specific access issues, such as those pertaining to Pharmaceutical, will be addressed in separate FAQs dealing with those sectors.**~~